

## CLAIMS:

1        1.        A method for detecting modifications to code placed in memory by the Power  
2        On Self Test (POST) Basic Input/Output System (BIOS) comprising the steps of:  
3                initiating said POST operation;  
4                retrieving code from a flash memory;  
5                measuring said retrieved code to generate a first measurement;  
6                storing said first measurement in a secure area;  
7                storing said retrieved code in a memory located in a non-secure area;  
8                measuring said retrieved code stored in said memory located in said non-  
9        secure area after receiving an awakening event to generate a second measurement;  
10       and  
11               indicating said retrieved code stored in said memory was modified if said first  
12       measurement is not equal with said second measurement.

1        2.        The method as recited in claim 1 further comprising the step of:  
2                awakening a system if said first measurement is equal with said second  
3        measurement.

1        3.        The method as recited in claim 1, wherein said indication comprises an error  
2        message.

1        4.        The method as recited in claim 1 further comprising the step of:  
2                rebooting a system thereby restoring said retrieved code to its proper values.

1        5.        The method as recited in claim 1, wherein said retrieved code comprises one  
2        or more of the following: legacy BIOS code and code used to support said legacy  
3        BIOS code.

1        6.        The method as recited in claim 5, wherein said code used to support said  
2        legacy BIOS code comprises one or more of the following: Universal Serial Bus  
3        (USB) interface support code and code for power management routines.

1       7.     The method as recited in claim 1, wherein said secure area is located within a  
2     trusted building block of a system.

1       8.     The method as recited in claim 1, wherein said secure area comprises a  
2     lockable Electrically Erasable Programmable Read Only Memory (EEPROM)  
3     module.

1       9.     A computer program product embodied in a machine readable medium for  
2     detecting modifications to code placed in memory by the Power On Self Test (POST)  
3     Basic Input/Output System (BIOS) comprising the programming steps of:  
4         initiating said POST operation;  
5         retrieving code from a flash memory;  
6         measuring said retrieved code to generate a first measurement;  
7         storing said first measurement in a secure area;  
8         storing said retrieved code in a memory located in a non-secure area;  
9         measuring said retrieved code stored in said memory located in said non-  
10    secure area after receiving an awakening event to generate a second measurement;  
11    and  
12         indicating said retrieved code stored in said memory was modified if said first  
13    measurement is not equal with said second measurement.

1       10.    The computer program product as recited in claim 9 further comprising the  
2     programming step of:  
3         awakening a system if said first measurement is equal with said second  
4     measurement.

1       11.    The computer program product as recited in claim 9, wherein said indication  
2     comprises an error message.

1       12.    The computer program product as recited in claim 9 further comprising the  
2     programming step of:  
3         rebooting a system thereby restoring said retrieved code to its proper values.

1       13.    The computer program product as recited in claim 9, wherein said retrieved  
2       code comprises one or more of the following: legacy BIOS code and code used to  
3       support said legacy BIOS code.

1       14.    The computer program product as recited in claim 13, wherein said code used  
2       to support said legacy BIOS code comprises one or more of the following: Universal  
3       Serial Bus (USB) interface support code and code for power management routines.

1       15.    The computer program product as recited in claim 9, wherein said secure area  
2       is located within a trusted building block of a system.

1       16.    The method as recited in claim 9, wherein said secure area comprises a  
2       lockable Electrically Erasable Programmable Read Only Memory (EEPROM)  
3       module.

1       17.    A system, comprising:  
2            a memory;  
3            a processor coupled to said memory;  
4            a first portion of a flash memory coupled to said processor, wherein said first  
5            portion of said flash memory comprises a Power On Self Test (POST) Basic  
6            Input/Output System (BIOS) code; and  
7            a Trusted Building Block (TBB) coupled to said processor, wherein said TBB  
8            is configured to ensure integrity of said system, wherein said TBB comprises:  
9                a second portion of said flash memory, wherein said second portion of  
10            said flash memory in said TBB comprises:  
11                a boot block code, wherein said boot block code comprises  
12            code to reset said system; and  
13                code to be moved from said second portion of said flash  
14            memory to said memory by said POST BIOS code during a POST operation;  
15            wherein said processor, responsive to said POST BIOS code, comprises:  
16                circuitry operable for retrieving said code from said second portion of  
17            said flash memory during said POST operation;  
18                circuitry operable for measuring said retrieved code to generate a first  
19            measurement;  
20                circuitry operable for storing said first measurement in a secure area;  
21            and  
22                circuitry operable for storing said retrieved code in said memory; and  
23            wherein said processor, responsive to said boot block code, comprises:  
24                circuitry operable for measuring said retrieved code stored in said  
25            memory after receiving an awakening event to generate a second measurement; and  
26                circuitry operable for indicating said retrieved code stored in said  
27            memory was modified if said first measurement is not equal with said second  
28            measurement.

1 18. The system as recited in claim 17, wherein said processor, responsive to said  
2 boot block code, further comprises:

3 circuitry operable for awakening said system if said first measurement is equal  
4 with said second measurement.

1 19. The system as recited in claim 17, wherein said indication comprises an error  
2 message.

1 20. The system as recited in claim 17, wherein said processor, responsive to said  
2 boot block code, comprises:

3 circuitry operable for rebooting said system thereby restoring said retrieved  
4 code to its proper values if said first measurement is not equal with said second  
5 measurement.

1 21. The system as recited in claim 17, wherein said retrieved code comprises one  
2 or more of the following: legacy BIOS code and code used to support said legacy  
3 BIOS code.

1 22. The system as recited in claim 21, wherein said code used to support said  
2 legacy BIOS code comprises one or more of the following: Universal Serial Bus  
3 (USB) interface support code and code for power management routines.

1 23. The system as recited in claim 17, wherein said secure area is located within  
2 said TBB.

1 24. The system as recited in claim 17 further comprising:  
2 a lockable Electrically Erasable Programmable Read Only Memory  
3 (EEPROM) module coupled to said processor, wherein said secure area comprises  
4 said lockable EEPROM module.